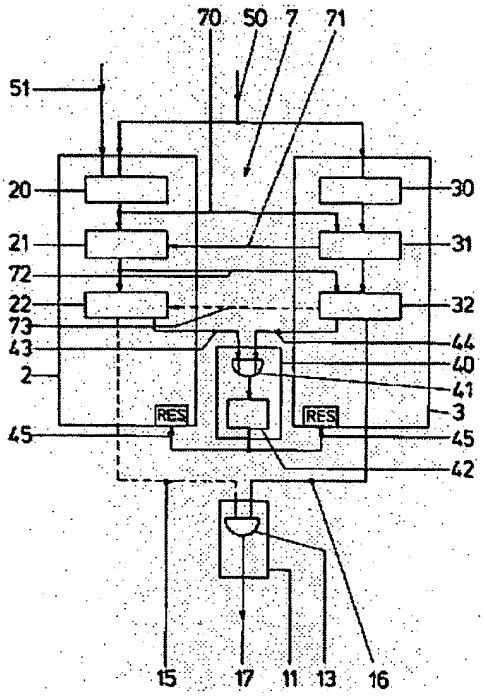
Vehicle safety system

Publication number: DE10032216
Publication date: 2002-01-24
Inventor: FUTTERLIEB ERNST (DE); HERMANN STEFAN (DE)
Applicant: SIEMENS AG (DE)
Classification:
- International: ***G05B9/02; G05B19/042;*** **G05B9/02; G05B19/04;** (IPC1-7): G05B19/048; G05B9/02
- European: G05B9/02; G05B19/042S
Application number: DE20001032216 20000703
Priority number(s): DE20001032216 20000703

Abstract of **DE10032216**

The vehicle safety system has a first and second program controlled units. The units are arranged to process the same safety program in dependence on signals of peripheral units. The input of at least one program controlled unit is connected to at least one peripheral unit. Functional units are arranged within the program controlled units. Each functional unit in the first program controlled unit has and is coupled to an associated functional unit in the other program controlled units. The corresponding functional units process the same program segment of the safety program. These provide a status signal in dependence on the relevant program segment which is sent to the following functional unit. In the case of a fault, a reset release signal is output. A reset unit is coupled to the output of the function units. This generates a reset signal to reset the program controlled units in dependence on reset signal fed to it indicating a fault.



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 32 216 A 1**

(51) Int. Cl.[7]:
G 05 B 19/048
G 05 B 9/02

(21) Aktenzeichen: 100 32 216.6
(22) Anmeldetag: 3. 7. 2000
(43) Offenlegungstag: 24. 1. 2002

DE 100 32 216 A 1

(71) Anmelder:
Siemens AG, 80333 München, DE

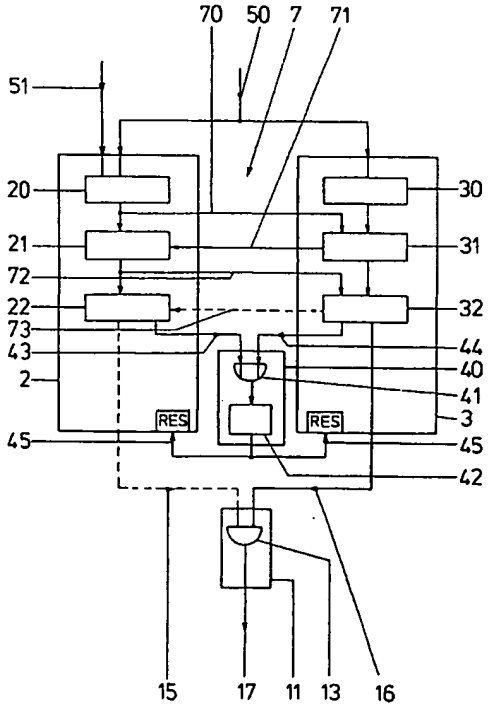
(72) Erfinder:
Futterlieb, Ernst, 93049 Regensburg, DE; Hermann, Stefan, 93096 Köfering, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Sicherheitssystem in einem Kraftfahrzeug und Verfahren

(57) Die Erfindung betrifft ein Sicherheitssystem in einem Kraftfahrzeug und ein Verfahren, bei dem ein Hauptrechner die Sensor- und Konfigurationseingänge steuert und diagnostiziert. Über einen SPI-Bus wird ein Schutzrechner eingangsseitig als Slave an den als Master fungierenden Hauptrechner angeschlossen. Der Schutzrechner überprüft den Zeitverlauf der Prozess-Signale, die vom Hauptrechner vorzugsweise über einen Prozess-Synchronisationsbus an den Schutzrechner herangeführt werden. Auf diese Weise ist ein anpassungsfähiges Sicherheitssystem mit konfigurierbarer Schutzfunktion realisierbar, die mit lediglich einer einzigen redundanten Hardwarekomponente (Schutzrechner) auskommt.



DE 100 32 216 A 1

Beschreibung

[0001] Die Erfindung betrifft ein Sicherheitssystem in einem Kraftfahrzeug sowie ein Verfahren zur Überwachung der ordnungsgemäßen Funktion eines Sicherheitssystems.

[0002] Sicherheitssysteme in Kraftfahrzeugen sind mit dem steigenden Bedürfnis nach mehr Sicherheit für die im Kraftfahrzeug zu schützenden Personen und Einrichtungen aus dem Kraftfahrzeug nicht mehr wegzudenken. Derartige Sicherheitssysteme sind häufig mit Rückhaltemitteln, wie z. B. Fahrer- und Beifahrerairbags, Seitenairbags, Gurtstraffern, Überrollbügeln und dergleichen, ausgestattet.

[0003] Bei sicherheitskritischen Systemen, wie sie in der Automobilindustrie und in der Luftfahrtindustrie vorliegen, sind sehr hohe Sicherheitsanforderungen sowohl für die Hardware als auch die Software solcher Sicherheitssysteme gestellt. Ein Ausfallen oder eine Fehlfunktion eines Elementes des Sicherheitssystems muss definiert erkannt werden, ungeachtet, ob es sich hier um einen Hardwarefehler oder um einen Softwarefehler handelt. Solche Fehler können beispielsweise bei einem defekten Sensor- oder Konfigurationseingang, bei einem Ausfallen der Zeitbasis oder der Referenzspannung des Steuerrechners, einem Fehler im Programm, etc. vorliegen. Aus diesem Grund werden häufig redundante Hardwarekomponenten eingesetzt, um eine möglichst sichere Funktionsweise der Sicherheitssysteme zu gewährleisten.

[0004] Die einfachste Form der Hardwareredundanz besteht aus einem Mikroprozessorsystem und einem, dieses System überwachenden, sogenannten Watchdog-Timer. Dieser Watchdog-Timer erhält periodisch, d. h. innerhalb einer vorbestimmten Zeitspanne, ein Statussignal vom Mikroprozessor. Wenn dieses Signal durch einen Software- oder Hardwarefehler nicht zeitlich korrekt generiert wird, so wird das System vom Watchdog-Timer in einen sicheren Zustand gesteuert (fail safe), eine Fehlermeldung wird ausgegeben (failure identification) und der Mikroprozessor wird neu gestartet (reset). Der Vorteil dieses Sicherheitssystems besteht darin, dass der Mikroprozessor wie auch der Watchdog-Timer in einem Kraftfahrzeug ohnehin schon zur Steuerung verschiedener elektrischer und elektronischer Fahrzeugfunktionen, wie zum Beispiel Motorsteuerung, ABS, ESP, Klimaanlage, Fensterheber, etc., vorhanden ist und nicht erst bereitgestellt werden muss.

[0005] Ein solcher Watchdog-Timer besteht aus einem frei laufenden Zähler, der kurz vor seinem Überlaufen durch das aktuelle Programm zurück gesetzt wird. Ein Fehler im Sicherheitssystem kann also immer erst beim vollständigen Durchlaufen des Watchdog-Timers erkannt werden. Dieser Vorgang bis zum Überlaufen des Watchdog-Timers kann je nach Einstellung mitunter sehr lang sein. Diese mitunter sehr lange Zeitdauer, die vielleicht bei den oben genannten "üblichen" Überwachungstätigkeiten eines Mikroprozessor ausreichend sein können, sind jedoch bei einem sicherheitskritischem System nicht akzeptabel, da beispielsweise im Kraftfahrzeug das Auslösen eines Rückhaltemittels, wie z. B. der Zündpille für einen Airbag, möglichst verzögerungsfrei erfolgen muss.

[0006] Alternativ zu der genannten einfachsten Form einer Hardwareredundanz wären auch komplexere hardwareredundante Sicherheitssysteme denkbar, bei denen jeweils für ein Eingangssignal eine redundante Sicherheitskomponenten vorgesehen sind. Allerdings werden die Anforderungen an Sicherheitssysteme in Kraftfahrzeugen künftig stark zunehmen, um den Schutz der Fahrzeuginsassen weiter zu verbessern. Damit einhergehend wird gleichermaßen die Zahl der Rückhalteeinrichtungen und deren zugehörige Auslösemittel ansteigen. Gleiches gilt für die Sensor- und Konfigurationseinrichtungen. Dies bedeutet aber, dass eine der Anzahl der Peripherieeinrichtungen entsprechende Anzahl von redundanten Komponenten für die entsprechenden Eingangssignale bereitgestellt werden müssen. Damit werden aber die genannten komplexen Sicherheitssysteme sehr umfangreich, was aus ökonomischen Gründen häufig nicht akzeptabel ist.

[0007] Es ist daher die Aufgabe der vorliegenden Erfindung, ein Sicherheitssystem anzugeben, welches eine vergleichsweise hohe Sicherheit bietet und das gleichzeitig möglichst einfach und kostengünstig herstellbar ist. Ferner soll ein Verfahren zum Betreiben des Sicherheitssystems angegeben werden.

[0008] Die systembezogene Aufgabe wird erfindungsgemäß durch ein Sicherheitssystem mit den Merkmalen des Patentanspruchs 1 gelöst. Demgemäss ist ein Sicherheitssystem in einem Kraftfahrzeug vorgesehen,

- mit einer ersten und mindestens einer weiteren programmgesteuerten Einheit, die zur Abarbeitung eines gleichen Sicherheitsprogramms in Abhängigkeit von Signalen der Peripherieeinheiten ausgelegt sind, wobei mindestens eine programmgesteuerte Einheit eingangsseitig mit mindestens einer Peripherieeinheit gekoppelt ist,
- mit in den programmgesteuerten Einheiten angeordneten Funktionseinheiten, wobei jeweils einer Funktionseinheit in der ersten programmgesteuerten Einheit eine weitere Funktionseinheit in der(den) weiteren programmgesteuerten Einheit(en) zugeordnet ist, die miteinander gekoppelt sind, die jeweils ein gleiches Programmsegment des Sicherheitsprogramms abarbeiten, die ein Statussignal in Abhängigkeit von dem jeweils abgearbeiteten Programmsegment bereitstellen, welches der jeweils nachgeordneten Funktionseinheit zuführbar ist, und die bei einem Fehler ein Resetfreigabe-Signal erzeugen,
- mit einer Rücksetzeinrichtung, die mit den Ausgängen der Funktionseinheiten der programmgesteuerten Einheiten gekoppelt ist und die abhängig von solchen ihr zugeführten Resetfreigabe-Signalen, die eine fehlerhafte Funktion anzeigen, ein Rücksetzsignal zum Rücksetzen der programmgesteuerten Einheiten erzeugt.

[0009] Die verfahrensbezogene Aufgabe wird erfindungsgemäß durch ein Verfahren mit den Merkmalen des Patentanspruchs 12 gelöst.

[0010] Die erste programmgesteuerte Einheit (Hauptrechner) steuert und diagnostiziert die Sensor- und Konfigurationseingänge. Es wird dabei berücksichtigt, dass keine redundanten Aufnehmer für die Eingangsdaten eingesetzt werden, dafür wird die eingeschränkte Redundanz der Eingangsdaten berücksichtigt. Über den SPI-Bus wird die andere programmgesteuerte Einheit (Schutzrechner) eingangsseitig als Slave an den als Master fungierenden Hauptrechner angeschlossen. Der Schutzrechner überprüft den Zeitverlauf der Prozess-Signale, die vom Hauptrechner gesendet werden. Diese Prozess-Signale werden vorzugsweise über I/O-Ports und über den Prozess-Synchronisationsbus an den Schutzrechner herangeführt. Über diesen Prozess-Synchronisationsbus werden Daten – beispielsweise über verschiedene Zustände des Hauptrechners wie dessen Einschaltphase, Steuerung und Lesen der einzelnen Eingangsschnittstellen, Diagnose der wichtigsten Funktionseinheiten, Aufprallerkennung, Ansteuerung von Ausgängen, Abschaltphase – an den Schutzrechner gesendet. Diese Schutzfunktionen können über Software an die jeweiligen Verhältnisse

bzw. Anforderungen angepasst werden.

[0011] Auf diese Weise ist ein anpassungsfähiges Sicherheitssystem mit konfigurierbarer Schutzfunktion realisierbar, die mit lediglich einer einzigen zusätzlichen Hardwarekomponente, nämlich die Bereitstellung des Schutzrechners, auskommt. Es muss hier lediglich sichergestellt werden, dass die Rechenleistung des Schutzrechners an die, aus der Sicht der Schutzfunktion, erforderlichen Aufgaben angepasst wird, um dadurch den Aufwand des erfindungsgemäßen Sicherheitssystems möglichst gering zu halten. Es lässt sich dann ein Sicherheitssystem bereitstellen, dessen Gesamtkosten signifikant geringer als die Kosten der eingangs beschriebenen klassischen Lösungen sind, wohingegen eine deutliche Verbesserung der Schutzfähigkeit gewährleistet werden kann.

[0012] Weitere vorteilhafte Ausgestaltungen und Weiterbildungen des Erfindungsgedankens sind den Unteransprüchen sowie der Beschreibung unter Bezugnahme auf die Zeichnung entnehmbar.

[0013] Die Erfindung wird nachfolgend anhand der in den Figuren der Zeichnung angegebenen Ausführungsbeispiele näher erläutert. Es zeigt dabei:

[0014] **Fig. 1** das Blockschaltbild eines erfindungsgemäßen Sicherheitssystems mit parallel angeordneten programmgesteuerten Einheiten;

[0015] **Fig. 2** ein detailliertes Blockschaltbild der programmgesteuerten Einheiten entsprechend **Fig. 1**.

[0016] In allen Figuren der Zeichnung sind gleiche bzw. funktionsgleiche Elemente und Signale, sofern nichts anderes angegeben ist, mit gleichen Bezugszeichen versehen.

[0017] **Fig. 1** zeigt in einem Blockschaltbild die Grundstruktur eines erfindungsgemäßen Sicherheitssystems **1**. Das Sicherheitssystem **1** weist zwei programmgesteuerte Einheiten **2, 3** auf, von denen die erste programmgesteuerte Einheit **2** als Hauptrechner und die andere programmgesteuerte Einheit **3** als Schutzrechner ausgebildet ist. Der Hauptrechner **2** ist vorteilhafterweise derart ausgelegt, dass er neben der Verarbeitung der Programmabläufe für die Schutzfunktionen auch andere Programmabläufe, beispielsweise Steuerungs-, Regelungsfunktionen und Statusinformationen verarbeiten kann. Der Schutzrechner **3** ist typischerweise lediglich zur Verarbeitung von solchen Programmabläufen ausgelegt, die für die Schutzfunktion des Sicherheitssystems erforderlich sind. Es wäre jedoch auch denkbar, dass beide programmgesteuerte Einheiten **2, 3** als Hauptrechner ausgebildet sind und quasi eine Arbeitsteilung der zu verarbeitenden Programme vornehmen, wobei lediglich sicherheitsrelevante Programmabläufe von beiden programmgesteuerte Einheiten **2, 3** gemeinsam bearbeitet werden. Besonders vorteilhaft ist ferner, wenn die beiden programmgesteuerten Einheiten **2, 3** jeweils eine eigene Zeitbasis und ein eigenes Referenzpotential VDD aufweisen.

[0018] Ferner sind zwei, mit den programmgesteuerten Einheiten **2, 3** gekoppelte Peripherieeinheiten **4, 5** vorgesehen. Im vorliegenden Ausführungsbeispiel ist die eine Peripherieeinheit **4** als Sensor – beispielsweise als Aufprallsensor – ausgebildet, während die andere Peripherieeinheit **5** eine Konfigurationseinheit umfasst. In **Fig. 1** wurde lediglich eine einzige Sensoreinheit **4** und eine einzige Konfigurationseinheit **5** dargestellt; es sei jedoch schon an dieser Stelle darauf hingewiesen, dass ein Sicherheitssystem in einem Kraftfahrzeug typischerweise eine Vielzahl solcher Sensor- und Konfigurationseinheiten **4, 5** aufweist.

[0019] Die Peripherieeinheiten **4, 5** sind über eine synchrone Bus-Schnittstelle **6** mit den beiden programmgesteuerten Einheiten **2, 3** verbunden. Im vorliegenden Ausführungsbeispiel ist diese synchrone Schnittstelle **6** als serielle SPI-Schnittstelle (SPI = synchronous serial interface) ausgebildet. Eine SPI-Schnittstelle **6** ermöglicht eine schnelle serielle Datenübertragung von bis zu 1 Mbit/sec zwischen Kommunikationsteilnehmern bei Entfernungen bis ca. 15 m. Für eine vollduplexe Datenübertragung werden hier typischerweise zwei serielle Datenleitungen **8, 9** zur Übertragung eines Datensignals (MOSI, MISO) und eine Taktleitung **10** für den Systemtakt (CLK) benötigt. Die programmgesteuerten Einheiten **2, 3** und die Peripherieeinheiten **4, 5** weisen hierfür entsprechende Ein-/Ausgänge MOSI, MISO, CLK auf.

[0020] Ein Kommunikationsteilnehmer, im vorliegenden Beispiel der Hauptrechner **2**, arbeitet als Master, der den Takt für die Datenübertragung nach dem Schieberegister-Prinzip bereitstellt. Der andere Kommunikationsteilnehmer, hier der Schutzrechner **2**, fungiert als Slave, der auf eine Masteranforderung seine Daten ausgibt. Da jeder SPI-Kommunikationsteilnehmer über ein Aktivierungspin (in **Fig. 1** nicht dargestellt) verfügt, lassen sich damit sehr einfach busähnliche Strukturen aufbauen. Obgleich eine derartige SPI-Schnittstelle **6** aus den genannten Gründen sehr vorteilhaft ist, sei die Erfindung jedoch nicht auf die Verwendung einer SPI-Schnittstelle **6** eingeschränkt, vielmehr sind auch andere Bus-Schnittstellen, wie z. B. ein I^2C-Bus, ein CAN-Bus oder dergleichen, denkbar. Ferner soll die Erfindung nicht auf serielle Schnittstellen beschränkt sein, vielmehr wäre auch eine parallel Schnittstelle von Vorteil.

[0021] Ferner ist ein Synchronisationsbus **7** vorgesehen, der zwischen den programmgesteuerten Einheiten **2, 3** angeordnet ist und der der Synchronisation der Datenkommunikation zwischen den beiden programmgesteuerten Einheiten **2, 3** dient. Die Funktionsweise des Synchronisationsbusses **7** wird nachfolgend noch anhand von **Fig. 2** detailliert erläutert.

[0022] Schließlich weist das Sicherheitssystem **1** zwei Ausgabeeinheiten **11, 12** auf. Im einfachsten Fall können die Ausgabeeinheiten **11, 12** als UND-Gatter **13, 14** realisiert sein. Die Ausgabeeinheiten **11, 12** sind mit den jeweiligen Ausgängen der programmgesteuerten Einheiten **2, 3** kreuzverschaltet. Über Verbindungsleitungen sind den Ausgabeeinheiten **11, 12** Freigabesignale **15, 16** zuführbar. Den Ausgabeeinheiten **11, 12** können in **Fig. 1** nicht dargestellte Rückhaltemittel, beispielsweise die Zündpille eines Airbags, die über einen Freigabebefehl **17, 18** ausgelöst werden, nachgeordnet sein.

[0023] **Fig. 2** zeigt ein detailliertes Blockschaltbild der programmgesteuerten Einheiten **2, 3** entsprechend **Fig. 1**. Die programmgesteuerten Einheiten **2, 3** sind, wie bereits erwähnt, zur parallelen Abarbeitung desselben Sicherheitsprogramms ausgelegt. Im Ausführungsbeispiel in **Fig. 1** weist der Hauptrechner **2** drei Funktionseinheiten **20, 21, 22** auf, die jeweils zur Abarbeitung eines einzelnen Programmsegmentes, das Teil des Sicherheitsprogramms ist, ausgelegt sind. Der Schutzrechner **3** weist eine gleiche Anzahl Funktionseinheiten **30, 31, 32** auf, die weitestgehend identisch wie die Funktionseinheiten **20, 21, 22** aufgebaut sind und die entsprechende Programmsegmente des Sicherheitsprogramms abarbeiten. Die Funktionseinheiten **20, 21, 22; 30, 31, 32** sind jeweils über Verbindungsleitungen **70–73** des Synchronisationsbusses **7** miteinander gekoppelt. Durch die so ausgestaltete Hardwareredundanz, also durch das Bereitstellen doppelt vorhandener und miteinander gekoppelter Hardwareelemente, wird eine hardwaremäßige oder softwaremäßige Fehlfunktion sicher erkannt.

[0024] Ferner ist in **Fig. 2** eine Rücksetzeinrichtung **40** vorgesehen, die eingangsseitig mit den Funktionseinheiten **20, 21, 22; 30, 31, 32** und ausgangsseitig mit den Reset-Eingängen RES der programmgesteuerten Einheiten **2, 3** gekoppelt ist. Die Rücksetzeinrichtung **40** weist ein ODER-

Gatter **41** sowie eine dem ODER-Gatter **41** nachgeschaltete Reset-Schaltung **42** auf. Über Verbindungsleitungen ist dem ODER-Gatter ein Resetfreigabe-Signal **43**, **44** zuführbar. Bei Vorliegen der entsprechenden Reset-Bedingungen erzeugt die Reset-Schaltung **42** ein Resetfreigabe-Signal **45**, das den programmgesteuerten Einheiten **2**, **3** zugeführt wird. Die Reset-Schaltung **42** könnte beispielsweise auch durch einen Watchdog-Timer bzw. einen Trigger-Watchdog ausgebildet sein. g

[0025] Nachfolgend wird die Funktionsweise der miteinander gekoppelten programmgesteuerten Einheiten **2**, **3** detailliert beschrieben:

[0026] Das Grundprinzip des erfindungsgemäßen Sicherheitssystems **1** besteht in der Bereitstellung zweier, in Bezug auf die Schutzfunktionen gleichberechtigter programmgesteuerter Einheiten **2**, **3**. Eine Entscheidung des Gesamtsystems, beispielsweise das Auslösen eines Airbags oder eines Überrollbügels, muss daher auch von beiden programmgesteuerten Einheiten **2**, **3** gleichzeitig getragen werden. Zu diesem Zweck werden alle sicherheitskritischen Eingangsdaten **50**, d. h. solche Eingangsdaten, die für die Schutzfunktion relevant sein könnten, in beide programmgesteuerte Einheiten **2**, **3** eingekoppelt und dort zumindest auf ihre Gültigkeit überprüft. Sicherheitsunkritische Eingangsdaten **51** werden hingegen lediglich in eine programmgesteuerten Einheiten **2**, **3**, im vorliegenden Fall in den Hauptrechner **2**, eingekoppelt.

[0027] Ferner wird jede programmgesteuerte Einheit **2**, **3** über die Vorgänge in der jeweils anderen programmgesteuerten Einheit **2**, **3** informiert und überprüft die Reihenfolge und die Zeitdauer der durch die jeweiligen Funktionseinheiten **20**, **21**, **22**; **30**, **31**, **32** bearbeiteten Programmsegmente. Beide programmgesteuerten Einheiten **2**, **3** können bei einer identifizierten festgestellten Fehlfunktion über ein Reset-Signal **45** beide programmgesteuerte Einheiten **2**, **3** zurücksetzen. Das Reset-Signal **45** wird hier über die Reset-Schaltung **42**, die beispielsweise von dem Hauptrechner **2** getätigt und gesetzt wird, erzeugt. Vorteilhafterweise kann der Schutzrechner **3** jedoch das Setzen der Reset-Schaltung **42** verhindern und somit das Reset-Signal **45** selber auslösen. Zu diesem Zweck ist die Reset-Schaltung **42** und die vorgeschaltete ODER-Schaltung **41** jeweils mit den Ausgängen der Funktionseinheiten **20**, **21**, **22**; **30**, **31**, **32** verbunden, die jeweils ein Freigabe- bzw. Statussignal über den Ablauf der von ihnen jeweils bearbeiteten Programmsegmente an die Rücksetzeinrichtung **40** sendet.

[0028] Die Statussignal auf den Verbindungsleitungen können je nach Anwendung ein unterschiedliches Format aufweisen. Eine mögliche Bitstruktur der Statussignale auf den Verbindungsleitungen **70–73** gemäß **Fig.** 2 wird nachfolgend anhand von **Fig.** 3 näher beschrieben:

[0029] Im einfachsten Fall reicht hier ein 3-bit breites Statussignal aus, um den ordnungsgemäßen oder ein fehlerhaften Betrieb zu erkennen. Ein solches Statussignal hat das Format "x1; x2; x3", wobei mit x1 das höchstwertige Bit (sog. MSB-Bit) und mit x3 das niedrigstwertige Bit (sog. LSB-Bit) bezeichnet ist. Das MSB-Bit x1 gibt im vorliegenden Beispiel an, von welcher programmgesteuerten Einheit **2**, **3** das jeweilige Statussignal stammt. Das x2-Bit zeigt das Ende eines Programmsegmentes an, während das LSB-Bit x3 anzeigt, ob dieses Ende jeweils erkannt wurde.

[0030] Den beiden Funktionseinheiten **20**, **30** werden jeweils kritische Eingangsdaten **50** zugeführt, die in den Funktionseinheiten **20**, **30** ein gleiches Programmsegment durchlaufen. Funktionseinheit **20** sendet den Funktionseinheiten **21**, **31** über die Verbindungsleitung **70** ein Statussignal, das das Ende des ersten Programmsegmentes anzeigt. Funktionseinheit **31** sendet daraufhin über Verbindungsleitung **71** seinerseits ein Statussignal, dass das Ende des ersten Programmsegmentes erkannt wurde. In der zweiten Stufe zeigt Funktionseinheit **21** den Funktionseinheiten **22**, **32** über die Verbindungsleitung **72** das Ende des zweiten Programmsegmentes an. Aufgrund eines software- oder hardwaremäßigen Fehlers konnte Funktionseinheit **32** jedoch das Ende des zweiten Programmsegmentes nicht erkennen, so dass der Funktionseinheit **22** ein entsprechendes negatives Statussignal übermittelt wird, was in **Fig.** 2 durch die gestrichelte Verbindungsleitung **73** dargestellt wurde. Von dem Hauptrechner **2** wird deshalb kein Freigabesignal **15** ausgegeben. Gleichzeitig erzeugt der Hauptrechner **2** ein Resetfreigabe-Signal **43**. Die Reset-Schaltung **42** setzt daraufhin über das Resetsignal **45** die beiden programmgesteuerten Einheiten **2**, **3** zurück.

[0031] Auf diese Weise kann eine Fehler – beispielsweise der Ausfall irgendeiner Funktionseinheit inklusive der Versorgungsspannungseinheit – bereits am Ende jeder ein Programmsegment ausführenden Funktionseinheit **20**, **21**, **22**; **30**, **31**, **32** erkannt werden und nicht erst nach einer vorbestimmten Zeitdauer der Reset-Schaltung **42**. Dadurch ist eine Echtzeit-Fehlererkennung möglich. Darüber hinaus wird auch eine softwareseitige Fehlfunktion definiert erkannt, wodurch der ganze Entwicklungs- und Prüfprozess signifikant verbessert wird.

[0032] Wie bereits erwähnt beschreibt das Ausführungsbeispiel gemäß **Fig.** 3 ein einfache Ausgestaltung des Busprotokoll auf dem Synchronisationsbus **7**. Es wäre jedoch auch denkbar und ggf. je nach Anwendung auch vorteilhaft, ein komfortableres Busprotokoll zu verwenden, das beispielsweise auch die folgenden zusätzlichen Informationen liefert:

- Art des Fehlers, z. B. Software- oder Hardwarefehler, Fehler in der Referenzspannung oder Taktversorgung;
- Umfang des Fehlers, d. h. wird dadurch die Funktionsfähigkeit des Sicherheitssystem beeinträchtigt;
- In welcher Funktionseinheit ist der Fehler entstanden; etc.

[0033] Ferner wurden im vorliegenden Ausführungsbeispiel die Resetfreigabe-Signale jeweils als 1-Bit breite Signale beschrieben, die bei einer "1" die nachgeordnete Schaltung **40**, **11** freigeben, wodurch ein Zündimpuls **17** oder ein Resetsignal **45** ausgelöst wird. Bei einer "0" wird die nachgeordnete Schaltung **40**, **11** gesperrt, dass heißt es wird kein Zündimpuls **17** oder Resetsignal **45** ausgelöst. Denkbar wäre jedoch auch hier, dass die Signale eine Bitbreite größer als eins aufweisen. Damit wäre es möglich, dass bei einem Fehler das System je nach Fehlertyp ein unterschiedliches Verhalten zeigt. Ein solches System kann abhängig von der Bitzahl des Signals **43**, **44**; **15**, **16** beispielsweise ein oder mehrere der folgenden Fehlerverhalten zeigen:

- Keine Vorkehrungen für den Ausfall des Systems;
- Identifikation und Anzeigen des Fehlers (failure identification);
- Umschalten in einen definierten, sicheren Zustand bei Auftreten eines Fehlers (Fail Safe; zum Beispiel bei einem Airbag-System;
- Bereitstellung einer Minimalfunktionalität (Limb Home; zum Beispiel bei einem ABS-System);
- Voll Funktionalität auch im Falle eines Fehlers (Failure Redundant, Fail Operational; zum Beispiel bei einem Satellitensystem).

[0034] Die Erfindung wurde anhand eines Sicherheitssystems im Kraftfahrzeug beschrieben. Jedoch sei die Erfindung nicht ausschließlich auf solche Anwendungen beschränkt; vielmehr ist sie vorteilhafterweise bei sämtlichen Sicherheitssystemen anwendbar, so zum Beispiel bei Sicherheitssystemen für die Luft- und Raumfahrtechnik sowie für Satellitensysteme. Die Erfindung eignet sich insbesondere für sehr komplexe Sicherheitssysteme mit einer Vielzahl von eingangsseitigen Sensor- und Konfigurationseinheiten und ausgangsseitigen Rückhaltemitteln.

[0035] Im vorliegenden Ausführungsbeispiel wurde das Sicherheitssystem der Einfachheit halber anhand einer einzigen redundanten Hardwarekomponente beschrieben. Selbstverständlich ließen sich, wenn dies erforderlich wäre, weitere programmgesteuerte Einheiten parallel anordnen, wodurch die Sicherheit bei der Erkennung einer Fehlfunktion noch erheblich gesteigert werden könnte.

[0036] Zusammenfassend kann festgestellt werden, dass durch das wie beschrieben aufgebaute Sicherheitssystem ein für die Zwecke einer möglichst hohen Sicherheit gegen Fehlfunktion optimiertes System bereitgestellt wird, ohne dass gleichzeitig die Nachteile von Sicherheitssystemen nach dem Stand der Technik in Kauf genommen werden müssen. Insbesondere bei sehr komplex ausgestalteten Sicherheitssystemen, beispielsweise mit einer Vielzahl von eingangsseitigen Sensor- und Konfigurationseinheiten und ausgangsseitigen Rückhaltemittel, lässt sich das erfindungsgemäße Sicherheitssystem durch die Bereitstellung lediglich einer redundanten Hardwarekomponente denkbar einfach und somit kostengünstig implementieren.

[0037] Die vorliegende Erfindung wurde anhand der vorstehenden Beschreibung so dargelegt, um das Prinzip und dessen praktische Anwendung bestmöglichst zu erklären. Selbstverständlich lässt sich die vorliegende Erfindung im Rahmen des fachmännischen Handelns und Wissens in geeigneter Weise in mannigfaltigen Ausführungsformen und Abwandlungen realisieren.

Patentansprüche

1. Sicherheitssystem in einem Kraftfahrzeug
mit einer ersten und mindestens einer weiteren programmgesteuerten Einheit (2, 3),
die zur Abarbeitung eines gleichen Sicherheitsprogramms in Abhängigkeit von Signalen (50) der Peripherieeinheiten (4, 5) ausgelegt sind,
wobei mindestens eine programmgesteuerte Einheit (2, 3) eingangsseitig mit mindestens einer Peripherieeinheit (4, 5) gekoppelt ist,
mit in den programmgesteuerten Einheiten (2, 3) angeordneten Funktionseinheiten (20, 21, 22; 30, 31, 32),
wobei jeweils einer Funktionseinheit (20, 21, 22) in der ersten programmgesteuerten Einheit (2) eine weitere Funktionseinheit (30, 31, 32) in der(den) weiteren programmgesteuerten Einheit(en) (3) zugeordnet ist,
die miteinander gekoppelt sind,
die jeweils ein gleiches Programmsegment des Sicherheitsprogramms abarbeiten,
die ein Statussignal in Abhängigkeit von dem jeweils abgearbeiteten Programmsegment bereitstellen, welches der jeweils nachgeordneten Funktionseinheit (20, 21, 22; 30, 31, 32) zuführbar ist, und
die bei einem Fehler ein Resetfreigabe-Signal erzeugen (43, 44),
mit einer Rücksetzeinrichtung (40),
die mit den Ausgängen der Funktionseinheiten (20, 21, 22; 30, 31, 32) der programmgesteuerten Einheiten (2, 3) gekoppelt ist und
die abhängig von solchen ihr zugeführten Resetfreigabe-Signalen (43, 44), die eine fehlerhafte Funktion anzeigen, ein Rücksetzsignal (45) zum Rücksetzen der programmgesteuerten Einheiten (2, 3) erzeugt.

2. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet, dass die Rücksetzeinrichtung (40) ein über Resetfreigabe-Signale (43, 44) angesteuertes ODER-Gatter (41) sowie eine dem ODER-Gatter (41) nachgeschaltete die von Ausgangssignalen des ODER-Gatters (41) getriggert wird, aufweist.

3. Sicherheitssystem nach Anspruch 2, dadurch gekennzeichnet, dass die Reset-Schaltung (42) als Watchdog-Timer ausgebildet ist.

4. Sicherheitssystem nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass ein Synchronisationsbus (7) vorgesehen ist, der zwischen den programmgesteuerten Einheiten (2, 3) angeordnet ist und der dazu ausgelegt ist, Statussignale jeweils gleicher Funktionseinheiten (20, 21, 22; 30, 31, 32) miteinander zu synchronisieren.

5. Sicherheitssystem nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass mindestens eine Ausgabeeinrichtung (11, 12) vorgesehen ist, die mit den Ausgängen der programmgesteuerten Einheiten (2, 3) gekoppelt ist und die abhängig von ihr zugeführten weiteren Freigabesignalen (15, 16) ein Freigabebefehl (17) zum Auslösen mindestens eines Rückhaltemittels erzeugt.

6. Sicherheitssystem nach Anspruch 5, dadurch gekennzeichnet, dass eine Ausgabeeinrichtung (11, 12) jeweils ein UND-Gatter (13, 14) aufweist.

7. Sicherheitssystem nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass eine programmgesteuerte Einheiten (2, 3) eine eigene Zeitbasis und/oder ein eigenes Referenzpotential (VDD) aufweist.

8. Sicherheitssystem nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass die programmgesteuerten Einheiten (2, 3) eingangsseitig über eine synchrone Schnittstelle (6) miteinander und mit mindestens einer Peripherieeinheit (4, 5) gekoppelt sind, wobei jeweils die erste programmgesteuerte Einheit (2) als Master und die weiteren programmgesteuerten Einheiten (3) als Slave konfiguriert sind.

9. Sicherheitssystem nach Anspruch 8, dadurch gekennzeichnet, dass die synchrone Schnittstelle (6) eine sogenannte serielle Peripherieschnittstelle (SPI) ist.

10. Sicherheitssystem nach Anspruch 8, dadurch gekennzeichnet, dass die synchrone Schnittstelle (6) an einem sogenannten Inter Integrated Circuit Bus (I^2C-Bus) angekoppelt ist.

11. Sicherheitssystem nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, dass mindestens eine Peripherieeinheit (4, 5) einen Sensor (4), insbesondere einen Aufprallsensor, und/oder mindestens eine Peripherieeinheit (4, 5) eine Konfigurationseinheit (5) aufweist.

12. Verfahren zur Überwachung der ordnungsgemäßen Funktion eines Sicherheitssystems nach einem der vorstehenden Ansprüche.

Hierzu 3 Seite(n) Zeichnungen

Nummer: DE 100 32 216 A1
Int. Cl.[7]: G 05 B 19/048
Offenlegungstag: 24. Januar 2002

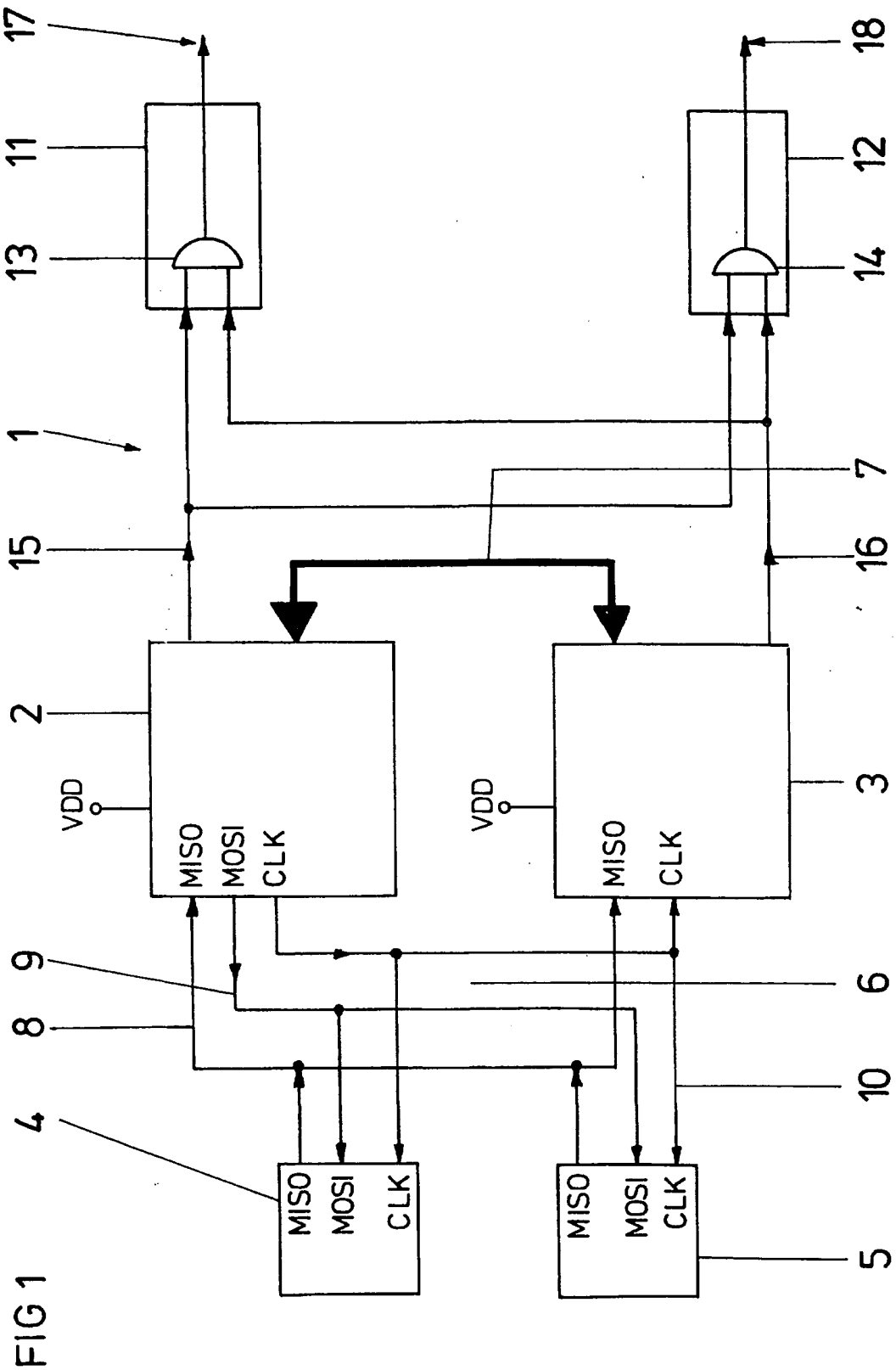
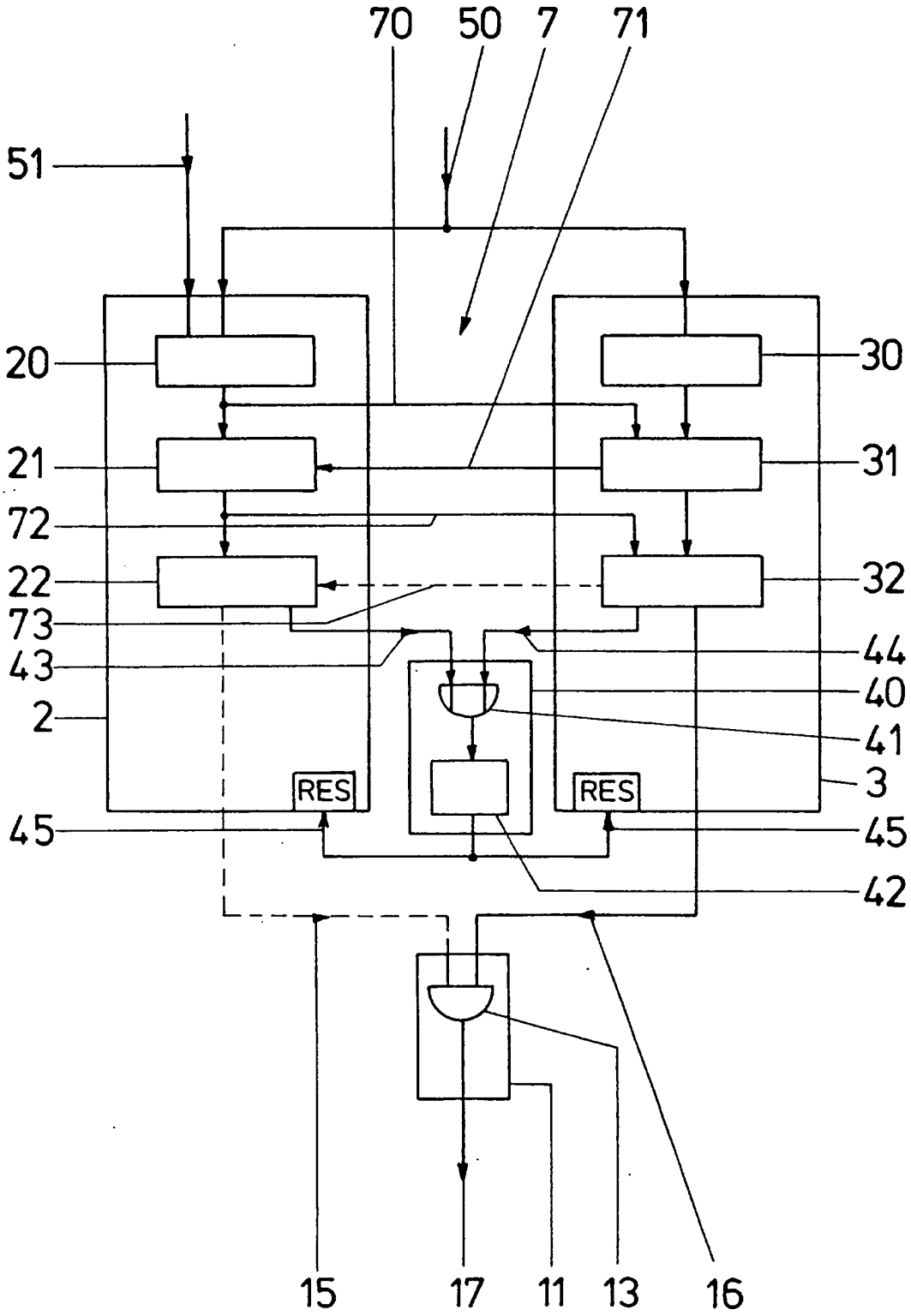


FIG 1

Nummer: DE 100 32 216 A1
Int. Cl.[7]: G 05 B 19/048
Offenlegungstag: 24. Januar 2002

FIG 2



Nummer: DE 100 32 216 A1
Int. Cl.[7]: G 05 B 19/048
Offenlegungstag: 24. Januar 2002

FIG 3